



# Internet and Data Security Essentials

Identify Threats To Your Privacy and Learn How You  
Can Protect Yourself



A Q Wealth Special Report  
By: John Harper

in association with [SecureLaptop.org](http://SecureLaptop.org)

## How To Protect Your Privacy Online- Internet and Data Security Essentials

© 2009 Q Wealth Limited, Port Vila, Vanuatu – All rights reserved

This guide contains confidential proprietary information and is not designed for the general public. It is produced exclusively for paid-up members of *The Q Wealth Report* for their exclusive personal and private use and knowledge, and under their own responsibility as sophisticated investors. Using or disseminating this information for any other purpose other than for what it is intended is a breach of copyright which may be subject to criminal and civil penalties, including imprisonment.

### **Q Wealth Communications Office:**

+44 20 3384 1993 UK and Rest of World

1-866-394-8944 USA and Canada

info@qwealthreport.com

### **Q Wealth Report Website**

<http://www.qwealthreport.com>

### **Secure Laptops Website**

<http://www.securelaptop.org>

## Table of Contents

<b>Chapter 1: How to Protect Yourself .....</b>	<b>5</b>
Secure your assets.....	5
Uncovering Potential Threats.....	5
Determining Risk.....	5
Identifying your adversaries.....	6
Basic Security Lessons.....	6
<b>Chapter 2: Protect Your Computer.....</b>	<b>8</b>
Threats and Adversaries.....	8
<i>Searches and Seizures.....</i>	<i>8</i>
<i>Subpoenas .....</i>	<i>11</i>
Protecting Yourself .....	11
<i>Establish A Data Retention Policy .....</i>	<i>11</i>
<i>Clear Web Browser Log.....</i>	<i>12</i>
<i>Delete Instant Messages.....</i>	<i>12</i>
<i>Implement The Retention Policy .....</i>	<i>12</i>
<i>Require Passwords .....</i>	<i>12</i>
<i>Encrypt Data.....</i>	<i>13</i>
<i>Protect Against Malware.....</i>	<i>13</i>
<b>Chapter 3 - Protecting Your Communications .....</b>	<b>14</b>
Threats and Adversaries.....	14
<i>Wiretapping .....</i>	<i>14</i>
<i>Pen Registers/Trap and Trace Devices .....</i>	<i>16</i>
What Can I Do to Protect Myself.....	17
<i>Protection against wiretaps.....</i>	<i>17</i>
<b>Chapter 4 - Information Stored by Third Parties.....</b>	<b>20</b>
Threats and Adversaries.....	20
<i>Government Subpoenas for Basic Subscriber Information.....</i>	<i>20</i>
<i>Government Search Warrants and “D” Orders .....</i>	<i>20</i>
<i>Unprotected Third Party Information About You .....</i>	<i>21</i>
<i>Communication Content Stored by Your Communications Providers.....</i>	<i>21</i>
What Can I Do To Protect Myself .....	22
<i>Landline Telephone Calls Are The Safest Communication.....</i>	<i>22</i>
<i>Protecting Your Email .....</i>	<i>23</i>
<i>Protecting Online Storage of Private Data .....</i>	<i>24</i>
<i>Protecting Your Search Privacy and Web Browser Activity .....</i>	<i>25</i>
<i>Don’t Use Your Cell Phone.....</i>	<i>25</i>
Encryption Basics .....	26

## How To Protect Your Privacy Online- Internet and Data Security Essentials

<i>Encrypting Your Data</i> .....	26
Web Browser Security.....	27
<i>Controlling and Limiting Logs Kept by Your Browser</i> .....	27
Secure Email Addresses.....	28
<i>Encrypting emails</i> .....	29
<i>Email Data Retention and Deletion Policy</i> .....	29
WiFi Security.....	30
Protecting Against Malware.....	30
Reduce the Risk of Malware.....	31
Using Tor to Hide Your IP Address .....	31
Secure Virtual Private Networks (VPN).....	32
Secure Virtual Over internet Protocol (VoIP).....	33
Personal Security Consulting.....	33
Conclusion.....	34

## Chapter 1: How to Protect Yourself

### **Secure your assets.**

You may not have thought about it but Information is one of your most valuable assets. Your emails, instant messages, data files and websites as well as the computers and servers holding all that information are assets to you and your organization. You need to protect these information assets just like you protect any other asset.

### **Uncovering Potential Threats.**

What are the threats to your information assets? Most often we think of protecting our information assets from being stolen and used by someone without our permission. In that instance, we are interested in protecting the confidentiality of our information and our control over who can see and use the information. However we need to also be vigilant against the threat of someone destroying our information assets or otherwise keeping us from being able to access our information assets. In this case we need to protect the integrity and availability of our information assets.

Encrypting information can protect the confidentiality, integrity and availability of your information assets and give you control over who can access the information.

Encryption scrambles the information so that only you or someone you intend to read it can. The scrambling protects the confidentiality of your information, gives you control over who can access the information and provides you with the added security of knowing that a person sending you information is who they say they are and provides confirmation that the information you send them or they send you has not been altered by an unauthorized person.

### **Determining Risk**

Risk is the likelihood of a threat occurring. The more likely the threat is of occurring the more we are willing to invest in protecting against the threat. If, for example, you live in a safe neighborhood with little crime the likelihood of someone breaking into your home is less than if you live in a crime ridden neighborhood where break ins are common. So you are more likely to invest in expensive locks and alarms if you live in the high risk neighborhood than if you live in the low risk neighborhood unless of course you

determine you have little of value to lose if someone does break in than maybe you will find even a high likelihood of a break in as acceptable.

Security measures you are willing to invest in are generally directly proportional in relation to the level of risk you perceive and the value of the assets you are trying to protect; the higher the level of risk of a threat occurring and the more valuable your assets the more you are willing to invest in security to prevent or minimize the threat.

Determining risk is a purely personal evaluation. Some risks are unacceptable to some people at any level of likelihood. Security decisions are a balancing of the value of the asset to you with the likelihood of the risk and the cost of the security measure.

An information asset example of risk evaluation is government privacy intrusions. Many worry about the risk of wiretaps or physical searches but most people are more at risk from a subpoena demanding records from you or your email provider than a wiretap or physical search of your property. That is why good data security practices are important. If your information is private don't give it to others to hold and don't keep it around but if you do have to store it protect it.

### **Identifying your adversaries.**

Knowing who your adversaries are helps to determine the appropriateness of your security solution. An adversary is anyone who poses a threat.

If your adversary is the government, business competitors, potential litigants who are interested in suing you or your company, hackers or organized criminals that are targeting you or your company or private investigators working for any of the above you need to encrypt your valuable information so your adversaries cannot read it if they get a hold of it.

Once you identify your adversaries you need to determine how much risk they pose to your information assets and then determine how you want to manage that risk. For example, if you consider the likelihood of the government secretly subpoenaing the contents of you email account from your webmail company a high risk you may decide to keep your emails on your own computer rather than the webmail company's server. In that instance you are trading the convenience of being able to access your emails from anywhere for the security of knowing no third party can turn over your emails to the government. Or you may leave your emails with the webmail company but encrypt the emails to protect the confidentiality of you information assets.

### **Basic Security Lessons.**

Before you make any critical security decisions here are a few basic security truisms you need to consider.

Your decisions are only as good as the information on which you are basing your decisions. If you do not have good information on the value of your assets, the severity of your threats to those assets, and the risk of the threats happening you will not necessarily make the “right” security decisions. Any security measure you take to protect your information assets is only as good as the weakest link in your communications system.

A simpler security measure is generally a safer security measure. Weaker links are easier to identify and correct in simpler security solutions. Simpler security measures are generally lower cost and have a lower risk of failure than complex security solutions.

More expensive security solutions are not necessarily more secure solutions. No security solution is perfect, there are always trade-offs.

You must continually re-evaluate and update your security solution. The security solution that works to protect today’s assets from today’s likely threats may not work to protect tomorrow’s assets from tomorrow’s likely threats.

**At SecureLaptop.org we offer personalized security consulting and training to not only educate you on what measures you should take for your data security, but also help you to choose the best services to make that happen.**

**From encrypted email addresses to totally secure military grade encryption laptops to offshore anonymous VPNs, we have all the resources necessary to ensure total privacy and security for your communications and information. Learn more here: <http://www.securelaptop.org/support-and-training.html>**

## Chapter 2: Protect Your Computer

This section reviews the potential threats of the government or others seizing your property or information. You will also learn how to protect yourself by protecting your confidential information from a search, seizure or subpoena or other potential threats.

### Threats and Adversaries

#### Searches and Seizures

The government is the most powerful and well funded adversary you need to worry about when assessing threats to your confidential information. The government's powers are limited by the Fourth Amendment's guarantee against **unreasonable** searches and seizures in places you have a **reasonable expectation of privacy**.

The courts have interpreted a seizure to include the government taking possession of items or detaining someone and searches to include any intrusion by the government into a place where you have a reasonable expectation of privacy – including your pockets, purse, luggage, laptop, cell phone, home, office, or hotel room.

If you are subjected to a search or threatened with a search by any government agent contact your lawyer immediately. If a search or seizure is found to be unreasonable the evidence obtained in the search or seizure cannot be used in a criminal proceeding.

##### a. Third Party Searches and Seizures of Your Information

An important limitation of the Fourth Amendment protections is created if you have knowingly shared your information with a third party. The courts have ruled that, for example, bank records including credit card records and telephone company records are not protected by the Fourth Amendment because you have knowingly communicated that information to a third party and thereby have assumed the risk

that they will share the information with the government. This is one very good reason to limit the information you freely share with third parties if you want that information to remain confidential.

### **b. Expectation of Privacy Exceptions**

You don't have a reasonable expectation of privacy if you throw something into the trash.

If your business, or a portion of your business, is open to the public you have no reasonable expectation of privacy in the public areas although if a government agent comes into your public areas you have the right to ask them to leave. Obviously there is no expectation of privacy in a public place like a sidewalk, park, store, or restaurant, or at a public gathering or meeting.

A virtual public place like an online social networking site has also been determined to be a public place with no reasonable expectation to privacy.

### **c. What the Government Must Do to Get a Search Warrant**

To conduct most lawful searches or seizures in a place where you have a reasonable expectation of privacy law enforcement must get a warrant from a judge or you have to consent to the search. A judge will issue a warrant only if there is evidence of probable cause. Probable cause has been defined to mean there is reason to believe the search will reveal evidence of a crime. The warrant must be specific as to where the search will take place and as to what the search is looking for.

### **d. Warrantless Searches**

There are a couple exceptions to the requirement for a warrant. One is the exigent circumstance rule. Exigent circumstances are emergency situations where it would be unreasonable for the police to wait to get a warrant, for example gun shots fired or someone calling for help. The other exception is the in plain view rule. The plain view rule allows the police to make a warrantless search or seizure if they are lawfully in a position to see and access the evidence, so long as that evidence is

obviously incriminating. While the plain view rule will not let the police enter your home or office without a warrant if they are already inside because you let them in or because of an exigent circumstance they can seize evidence that is in plain sight if they believe it is evidence of a crime. Law enforcement can search an automobile without a warrant if they have probable cause.

Airport and border searches are also legal without a warrant. Assume if you are traveling by plane or crossing a border you, your bags and anything else you are carrying will be searched. This includes the right to search the contents of your laptop. If you have confidential information on your laptop you may want to leave it at home.

#### **e. What To Do If You Are the Subject of a Warrant Search**

If law enforcement shows up at your door without a warrant do not consent to a search, do not invite them in (that might be an implied consent to a search) and do not leave the door open behind you if you walk out on the porch to talk to the officers (an open door could be an implied invitation to come in).

Ask politely to see the warrant. If the warrant seems accurate, has the correct address and Judge's signature, let them in and say, "I do not consent to this search." This will reserve your rights to challenge the search later.

A warrant does not require you to answer any questions. You have the right to an attorney before you answer any questions. Write down the police officer's name and badge number and anything the police say to you or you say to them. If possible watch the search and if they appear to go beyond the places authorized in the warrant politely point this out. At the end of the search ask for an inventory of anything they seize but do not sign any paper that suggests you agree the inventory is complete or accurate. As soon as possible call your lawyer.

If the warrant specifies your computer itself is evidence of a crime the police may seize it. If however the warrant specifies the data on the computer is possibly evidence of crime the law enforcement agents will likely print or make an electronic copy of the information stored on the computer.

## **Subpoenas**

The government or a private individual or entity involved in civil litigation can also obtain documents or information with a subpoena. A subpoena can require you to provide evidence about yourself or someone else and can require someone who has information about you to provide that to law enforcement. You have the opportunity to challenge a subpoena before you comply. If the judge agrees with your argument that the subpoena is too broad or unduly burdensome, is seeking privileged information or information protected by the First Amendment's protections of free speech he can quash the subpoena.

If you know about it you can also contest a subpoena directing a third party to provide information about you but often you are not notified of these subpoenas.

If you receive a subpoena contact your attorney immediately.

## **Protecting Yourself**

You can't protect yourself against your computer being seized by the government with a warrant and the best defense against a subpoena is a good lawyer but you can take action to limit the information the government or others can get off your computer.

### **Establish A Data Retention Policy**

If you don't want someone else to see it don't keep it. Establish a data retention policy defining whether and when different types of data should be destroyed. For example, you may choose to destroy computer files (don't just trash the files make sure they are being overwritten immediately after deletion) or paper documents (shred the paper documents and CD's) six months after you are done using the files. It is important you establish the retention policy in writing and follow the policy so you cannot be accused of hiding or destroying evidence. Never destroy documents or computer files after you receive a subpoena or you risk a criminal charge of destroying evidence.

## **Clear Web Browser Log**

Other actions you can take to protect yourself are to regularly clear out your web browser's history or sites you have visited and documents you have downloaded.

## **Delete Instant Messages**

Set your instant messaging software preferences so that your instant messages are deleted every so often and include this in your data retention policy. If you do save the instant messages for a period of time protect them with an encryption program (such as the one that comes standard with our [totally secure laptops](#) called Pidgin Instant Messenger with Off-the-Record encryption and more). Take these same precautions if you run a network or have an email or web server.

## **Implement The Retention Policy**

It doesn't do any good to establish a policy if everyone is not following the policy. Make your data retention policy a routine. Follow through once a day or once a week and make sure:

- All paper documents and CD's with documents scheduled to be destroyed have been shredded.
- Delete any emails or other documents that are scheduled for deletion under your policy.
- Clear your browser logs.
- Run your secure-deletion software to overwrite all of the deleted material.

## **Require Passwords**

Other defensive actions you can take to protect your computers and the data they store is to require log in passwords before the machine will allow access to a user account. Set the screen saver so that if the machine remains unused for a short period of time the password has to be reentered.

Require pass words to be complex. A phrase is better than a word and it should include upper and lower case letters and one or more numerical digits. Require that passwords

be changed frequently. Don't use the same password on multiple accounts. If possible don't write your passwords down. If you have multiple passwords and just can't remember them all there are software tools called password safes that will save your passwords on your computer in an encrypted form then you will only have to remember the password to the password safe.

## **Encrypt Data**

Even with password protected accounts all the government of anyone else has to do is take out your hard drive and stick it in another computer to open the files. That is where encrypting your files will buy you some time for your lawyer to contest the seizure, or limit the search to exclude legally protected files or negotiate a deal with the prosecutor. Only a judge can force you to provide your encryption password to the government (and the law is not entirely clear on that yet).

Encrypted data will also protect you against a sneak and peek searches. The government may have you data but they can't read it if it is encrypted.

## **Protect Against Malware**

While it is unclear if the government is using malware to access you computer almost every other hacker out there is. The threats include denial of service, and software or data theft and destruction and the hijacking of your computer to attack other computers and networks. The risk of this happening is high if you use the internet.

The best defense is to keep sensitive data on a computer that is not connected to the internet. Other suggestions are to avoid using Microsoft products they are especially vulnerable; keep your software updated; and maintain your firewall software and hardware.

**The secure laptops we offer at [SecureLaptop.org](http://www.securelaptop.org) come with everything you need to ensure your computer remains protected, encrypted, and safe. They come standard with military grade AES 256 encryption which is impossible to crack, a full software suite for encrypting and protecting your communications, a secure email address, your own Offshore VPN, and much more. See the details here: <http://www.securelaptop.org/totally-secure-laptops.html>**

## Chapter 3 - Protecting Your Communications

When the government wants to conduct surveillance of your communications they can plant a bug to eavesdrop, wiretap you phone and internet communications or use tracing devices to track those with whom you communicate. This section will review steps you can take to defend against surveillance.

### Threats and Adversaries

#### Wiretapping

The government and almost anyone else with a few hundred dollars has the technical capability to eavesdrop on your conversations be they face-to-face conversations, phone or email conversations or instant messages. The government has a sophisticated wiretapping system called "DCSNet" ("DCS" stands for "Digital Collection System") that is tied into key telecommunications switches across the country. This system is capable of intercepting wire-line phone calls, cellular phone calls, SMS text messages and push-to-talk communications, or to track a cell phone's location. The government is believed to have similar capabilities when it comes to Internet communications.

Technology has also made it easier to eavesdrop on your face-to-face conversations with the cooperation of your cell phone provider. This technology will convert the microphone on your cell phones into a bug. The government likely also has the ability, with your phone company's help, to open the line on your landline phone and use its microphone as a bug, and possibly, using remotely-installed government malware, to turn on the microphone or camera on your computer.

The technology exists for almost anyone to eavesdrop on anyone they want almost anywhere and anytime they chose. Use of the eavesdropping equipment is highly regulated and cannot be done legally without a court order. However, the government has, in the past, used wiretaps and other surveillance equipment without a court order. While information gathered from an illegal surveillance could not be used in a criminal prosecution there is no way to know how else it might be used against you.

The Federal Wiretap Act passed in 1968 requires law enforcement to get a court wiretap order whenever they want to intercept an oral communication, an electronic communication or a wire communication. According to the Wiretap Act it is a crime for anyone that is not a party to a communication to intercept the communication unless one of the parties has previously agreed to the interception or unless a wire tap order has been issued by the court.

Many state laws require all parties to a communication to consent to an interception however state laws only apply to local law enforcement and not the federal government.

It is important to point out that law enforcement does not need a wiretap order to go to your public website, MySpace or Facebook account, to read an email newsletter or join in and internet chat room dialogue. These are all public venues and do not therefore create a reasonable expectation of privacy.

To obtain a court wiretap order is not easy. The request must include information about the crime that is being or about to be committed, the place where the wiretap will be used and information about your phone company or internet service provider from which the communications will be intercepted. The request must also state what communications law enforcement is interested in intercepting, the identity of those committing the crime, those whose communications law enforcement is interested in intercepting and if previous wiretap orders have been issued for the same individuals. The government must also state that all other investigative procedures have been tried and failed or are too dangerous to try and finally the time period they are requesting the order to cover.

If the court issues a wiretap order it almost always requires the cooperation of a third party to initiate a wiretap. Usually the third party is your phone or internet service provider but it could be your landlord or hotel operator. The wiretap order usually includes a gag order prohibiting the third party from talking about the wiretap with you or anyone else.

Although you probably won't know when the wiretap order is issued there is a requirement that the government notify you of the communications intercepted after the order expires.

### **What is the risk of a wiretap**

The 2007 wiretap report to Congress stated 2,208 applications for wiretaps were submitted, including 457 federal requests. On average each wiretap intercepted over 3000 communications from over 94 individuals.....that means over 200,000 individual's communications were intercepted in 2007. Of the reported wiretaps most were on phones rather than electronic communications. That is likely because it is easier for the government to obtain your electronic communications through your internet service provider than through a wiretap.

So what is the risk of your communications being intercepted? The risk of your phone being tapped or your internet communications being intercepted are probably pretty low unless you associate with those suspected of drug dealings or those targeted for foreign intelligence surveillance than your risk increases.

### **Pen Registers/Trap and Trace Devices**

The Supreme Court determined in 1979 that the Fourth Amendment did not protect the numbers you call only the contents of your conversations so there is a much lower burden for the government to access the record the phone numbers you call. Basically law enforcement only has to state it is likely the dialing information will be relevant to a criminal investigation. A pen/trap on your phone will allow law enforcement to intercept the phone numbers you call and that call you, the time the calls are made, if the call connected or went to voicemail and the length of the call.

The USA Patriot Act expanded the use of pen/trap orders to intercept information about you internet connections. With a pen/trap order your internet service provider can be required to provide all email header information including email addresses of the people to whom you send email and the email addresses of those who send mail to you, the time of the email and the size of the email. The pen/trap also captures IP addresses and communication ports and products used. It is unclear if a pen/trap order is legally sufficient to allow the collection of information about particular pages you are visiting or files you are downloading or if the government needs a wiretap order to do that.

Once law enforcement has the email and IP addresses it is relatively easy to identify who you are communicating with based on that information.

The pen/trap also can capture “pings” from your cell phone to pinpoint the physical location of the phone.

### **What is the risk of Pen Registers/Trap and Trace Devices**

While there are no official requirements to report pen/trap surveillance there are unofficial reports that suggest as many as tens of thousands of the pen/trap orders are used annually making the risk of this type of surveillance higher than the risk of a wiretap.

## **What Can I Do to Protect Myself**

Your best defense is to use communications that possess the strongest legal protections like face-to-face conversations, postal mail and landline telephones. Since that is not always possible or desirable you can use encryption to protect your communications from being read if intercepted.

### **Protection against wiretaps**

#### **a. Face-to-face and Landline Communications Are Your Best Bet**

The most secure way to communicate is still face-to-face conversations or landline phones because the only way the government can legally eavesdrop on those conversations is with a court ordered wiretap which is difficult to obtain. And even if there is an illegal bug or tap on your landline any communications intercepted could not be used against you in a criminal trial.

If the conversation is particularly sensitive you may want to have a face-to-face conversation in a room without cell phones or computers with cameras or microphones to ensure that there are no remotely operated bugs recording your conversation. The trade off here is security versus convenience.

Even though your landline could be tapped and is statistically more likely to be tapped than your internet communications it is still less risky than internet communications. For one thing there is no copy of your phone conversation once the call is over whereas copies of your internet communications are around until you delete them making it easier for your adversary to access them sometime after the communication has taken place.

### **b. Cell Phones and Cell Phone Communications Are Risky**

Cell phone communications are highly vulnerable to interception both technically and legally. The calls and text messages made and received from your cell phone can be intercepted by almost anyone without the cooperation of the cell phone provider. There is a legal theory that cell phone communications do not enjoy a reasonable expectation of privacy and are therefore cell phone conversations and text messages may not be protected by the Fourth Amendment.

In addition cell phones can be used by your adversaries to track your location in some cases this can be done even if the phone is turned off. This tracking can be done without the providers assistance and in the government's case can be done with a pen/trap order rather than the legally more difficult to obtain wiretap order. This makes the threat of an adversary using your cell phone to pinpoint your location easy to do and the risk of location tracking fairly high. The best way to eliminate the risk is not to carry a cell phone. The trade off here is convenience versus security. A compromise may be to carry a cell phone but remove the battery except when the cell phone is needed.

Text messages are at a higher risk communication than cell phone conversations because text messages are classified as an "electronic communication" rather than a wire communications and therefore are not protected by the Wiretaps Act's exclusionary rule and the government could use an intercepted text message against you in a criminal case even if it was obtained without a wiretap order.

Considering all these risks and the lack of easily available encryption software for cell phone text messages the best bet is not to use text messages at all or if you use text messages only use them for the most routine communications.

### **c. Internet Communications pose the Highest Risk of Interception**

Access to your internet communications is easy and cheap and can be done by almost anyone. If you are using a wireless internet connection (WiFi) those communications are accessible to anyone in the area without specialized equipment or expertise. If a communication is sensitive do not send or receive it on a wireless connection.

The only way to protect your internet communications against being read by the government or anyone else is using an encryption system. An advantage of using encryption is that it not only protects your communications from being intercepted

when they are being sent it also protects the communications stored on your computer or stored by your internet service provider. Sure encryption systems can be broken but that requires effort and expertise. So while encryption is not a perfect solution it does increase your security significantly.

An encryption system will not protect you from pen/trap information being accessed from your communication. There are tools like Tor that allow you to send your internet communications anonymously by hiding your IP address which you might consider to lower this risk.

The trade off is increased communication security versus the inconvenience and expense of installing and using an encryption system. The trick here is to find easy to install and use encryption software.

**It is essential that all your sensitive communications be encrypted at all times. That is why at SecureLaptop.org we offer:**

- **Secure Email addresses (<http://www.securelaptop.org/secure-e-mail.html>)**
- **Secure VoIP services (<http://www.securelaptop.org/secure-voip.html>)**
- **Offshore VPNs (<http://www.securelaptop.org/encrypted-vpn.html>)**
- **Full Communication Encryption Suite on our secure laptops (<http://www.securelaptop.org/totally-secure-laptops.html>)**

**Using these measures ensures that your communications are as protected and encrypted as legally possible.**

## Chapter 4 - Information Stored by Third Parties

Phone companies, internet service providers, websites you visit and search engines all collect information about you everyday including: who you are calling, emailing or instant messaging; what web pages you are reading; and what information you are searching for online. In addition you are likely storing communications with these third parties like voice mail messages and emails.

### Threats and Adversaries

#### Government Subpoenas for Basic Subscriber Information

What information about you can the government legally obtain from third parties? With a subpoena the government can require communications providers to turn over “basic subscriber information.” This includes your name, address and length of time you have used that provider’s services. “Basic subscriber information” can also include local and long distance telephone call records, internet records indicating when you signed in and off the service, how long you were online each time and the IP address assigned to you each time you logged on and information on how you pay your bill including credit card or bank account information. Third party providers are usually ordered not to talk to you or anyone else about the subpoena and while the government must notify you of a subpoena they usually don’t until after they obtain the information.

#### Government Search Warrants and “D” Orders

To access any information other than “basic subscriber information” from your communications providers, the government must request a court to issue a search warrant or a “D” Order authorized by subsection (d) of section 2703 of the Stored Communications Act. “D” orders are easier to get than search warrants but more difficult to obtain than a subpoena. “D” orders can be issued with no notice to you and can restrict the provider from telling you or anyone else about the order.

The type of information the government may seek with a “D” order includes email addresses of those you send emails to and those who send emails to you and the size of the email; IP addresses you communicate with when you communicate with them and how much information you exchanged; and the addresses of web pages you visit. In the case of cell phone companies the government may want records with regard to which cell phone tower your phone was connecting to when you made calls which can help pinpoint your location at those times.

How long your communications provider keeps these types of records varies with the provider but typically providers will keep this information for at least several months.

## **Unprotected Third Party Information About You**

It is unclear if the Stored Communications Act extends any protections to records kept by the websites you visit or the web search engines you use. The law clearly includes communications providers but web sites and search engines do not provide a communication service. The type of information collected by websites and search engines includes requesting IP address, time of request, first line of the request, success or failure of the request, size of the response, previous page viewed by the requester and name and version of the web browser used.

## **Communication Content Stored by Your Communications Providers**

There are stronger protections accorded to the content of communications stored by your communications providers like emails, voice mails and instant messages. The third party providers are forbidden by law to share the contents of stored communications with anyone other than the government and then only with the appropriate order. It is important to note that if your email is delivered by a University or business email system and the University or business privacy policy does not provide otherwise the content of communications stored on these systems can be shared with the government at the discretion of the provider.

If the communications are unopened and have been in storage for less than 180 days law enforcement must get a search warrant to access the content. There is

one exception to this rule. That exception states if the provider believes in good faith that not immediately disclosing the communications could lead to someone's death or serious injury, they can provide the contents to the government without a warrant.

If your stored communications are opened or unopened and older than 180 days law enforcement only needs to obtain a "D" order or subpoena to require the third party to turn over the contents of the communications. Remember the requirement to notify you of a subpoena or "D" order does not specify a time of notification and almost always the notification is delayed.

There is some disagreement among the Appellate Courts as to whether an opened message in storage for 180 days or less can be obtained without a search warrant. The Ninth District Appeals Court (located in California) has taken a position that search warrants are required to access the contents of these communications suggesting that California based providers may offer users of their services greater protection than those providers in other parts of the country - at least until the Supreme Court rules on this issue.

For all of the reasons stated above it is preferable if you store communications on your own computer rather than with a third party since the government will always need a warrant to access information on your personal computer.

## **What Can I Do To Protect Myself**

Minimize your communications that are stored by third parties. It is easier for the government to gain access to communications stored by third parties than it is to obtain communications you have personally. If third parties do store some of your communications encrypt those communications. If you go online use software like Tor to do so anonymously. Consider using activist friendly communications providers like The Online Policy Group or Rise Up which offer free web and email hosting services with strong privacy policies.

## **Landline Telephone Calls Are The Safest Communication**

Telephone calls from a landline create no records of content for the communications provider to store and are therefore the safest form of communication since without a wiretap the government cannot access the content of you landline calls without the cooperation of the person with whom you are talking. If you have voice mail from a third party provider however the protections are much weaker. Where possible use you own answering machine not the phone companies. If you do use third party voice mail delete the messages as soon as you listen to them. Providers of voice over IP telephone services like Skype do not record calls so there are no stored copies of those calls for the government to obtain. The only risk of a voice over IP conversation is a wiretap,

## **Protecting Your Email**

Because of the government's aggressive position with regard to stored emails you need to be vigilant deleting emails from your third party provider's storage as soon as you access the messages. If you need to store incoming, sent or draft email content store the content locally on your computer. In either case encryption of your email is recommended.

Avoid using webmail at all or configure you email client software to send and receive emails directly via POP. The trade off of not using webmail is you will have less risk of the content being obtained by the government but you will sacrifice the convenience of being able to access your emails from external devices.

Stored web mail like Gmail and Yahoo mail is also at high risk of being obtained easily by law enforcement. It is easy for the government to obtain access to these stored communications by going to the third party provider. The convenience of web mail is probably not worth the risk if the information you are communicating is sensitive. If you must use web mail encryption is a good idea.

**At SecureLaptop.org we offer a Secure Email service which is simple, reliable, and totally secure an anonymous. You can learn more here:  
<http://www.securelaptop.org/secure-e-mail.html>**

## 1. Protecting Your Instant Messages

Instant message providers like AOL, Yahoo and Microsoft don't store instant messages but even so encrypting instant messages is easy, so do it. Gmail chat logs all your instant messages by default and stores them. If you use Gmail chat, turn off the storage feature by changing the default setting to an "off the record" setting. This solution will do you no good unless those you are chatting with also go "off the record."

Many cell phone providers claim they delete text messages within 72 hours after they are sent however in high profile cases older text messages have been made available to the government and sometimes with just a subpoena and not a warrant. Easy access to text messages makes them a high risk communication. There is also the added risk that text messages are being logged by both your provider and the provider of those with whom you are communicating. There are no reliable encryption solutions for text messages at this time so your best solution is not to text.

**Our totally secure laptops come with a communication encryption software suite which includes the Pidgin Instant Messenger with Off-The-Record encryption. You can learn more here: <http://www.securelaptop.org/totally-secure-laptops.html>**

## Protecting Online Storage of Private Data

Online calendars, contact lists and documents are stored by remote computing services regardless of how old they are can be accessed by the government with a subpoena. Although the government is required to notify you of the subpoena it is often after the fact. You are much more secure if you store this information on your personal computer. If you must use a remote computing service encrypt the data before you use these online services.

There is no expectation of privacy and therefore no protection to keep anyone including the government from accessing information you voluntarily publish on a blog, MySpace, Facebook, Twitter or other social networking sites.

## **Protecting Your Search Privacy and Web Browser Activity**

Before you use search engines or log on to a web site use a software like Tor to mask your IP address. Another good idea is to use multiple portals for your online services there is no need to make it easy for the government to access all types of personal information through one provider.

## **Don't Use Your Cell Phone**

The only way to avoid cell phone records from being used to track your locations is not to use a cell phone to make or receive calls. A partial solution may be to use prepaid cell phones purchased with cash. The location data will still be recorded but it will be harder to link to you.

At OffshoreLaptop.org we have multiple services to ensure that your 3<sup>rd</sup> party data is protected and secure: Encrypted Cloud Storage Offshore Routers Encrypted VPN Learning about these services will help you to protect your information when it is stored by 3<sup>rd</sup> parties.

## Chapter 5 - Security Options

This section outlines some of the steps you can take to secure your personal information including how to use disk encryption software, how to improve the security of your communication applications, how to reduce the threat of malware, and how to create virtual private networks. Before implementing any of the options discussed here you might want to review information from other sources as technology is constantly evolving and new products may be available.

### **Encryption Basics**

Encryption uses mathematical formulas to transform information into a code that is not readable unless you have the encryption key. If you encrypt your emails and information stored on your computer or third parties computers it will mitigate the threat of your sensitive data being accessed by those who don't have a key. You can also use an encryption program to protect yourself from others collecting your personal information when you use internet web browsers.

### **Encrypting Your Data**

The most effective way to eliminate threats of someone accessing sensitive data without your permission or knowledge is not to store it on your computer. If you have to store sensitive data on your computer you should use either disk encryption or a hard disk password or both to minimize the risk of someone accessing your information without your permission. If you want the highest level of security a use full disk encryption program and a hard disk password. You can chose to use a file encryption that only applies to certain specific files on your computer which may be easier but full disk encryption offers more protection.

There are many encryption tools. Using mainstream yet military grade products such as BitLocker, PGPDisk, FileVault, TrueCrypt and dm-crypt(LUKS) is recommended.

Once you have installed disk encryption software you will have to enter a separate disk password when you turn the computer on or start using the disk. If you use full disk encryption on your server you will not be able to do an unattended reboot because someone will have to enter the disk password whenever the computer is restarted.

It should be noted that encryption will stop unauthorized persons from reading your documents however it will not protect sensitive documents if you receive a subpoena requesting those documents in a civil litigation. If a judge in a civil case issues a subpoena for your data failure to decrypt that data would result in a contempt of court finding. The only sure way to protect data in a civil case is not to store it on your computer in the first place.

SecureLaptops.org makes totally secure laptops that are protected with a military grade and unhackable AES 256 encryption. We offer installation and support packages targeted to personal computers, small business computers and large corporate computer systems. See more about the services offered for totally secure visit us at: <http://www.securelaptop.org/totally-secure-laptops.html>

## **Web Browser Security**

Web browsers are software that connects your computer with other servers or hosts on the internet. Anytime you use a web browser it stores data on your computer and creates a log which is stored on the web servers you visit. This information can be accessed by any adversary that is monitoring your network connection unless you take steps to prevent the data from being collected and stored.

### **Controlling and Limiting Logs Kept by Your Browser**

Web browsers retain a history of the web pages visited, cached copies of the pages visited, information about accounts logged into and the names and data you enter into web forms. Web browsers also create cookies that record preferences and link your browser to third party web servers.

Cookies are the mechanism used to record a visitor logging into an account on a site and to track purchases that visitor makes. So, if you make purchases online you don't want to block all cookies all the time. Most browsers offer an optional setting that allows the cookies to be created for a single session and deleted when you quit the browser session.

You may also want to check out the "Incognito" mode offered by Google's Chrome browser and the "Inprivate" mode offered by Internet Explorer 8 for options to limiting cookie tracking.

Most web browsers also offer features to manage their stored data privacy settings but you have to enable the settings to delete or clear the browser history. Check your browser settings for each browser you use to ensure your information is cleared on a regular basis.

A new feature implemented by some browsers is a "flash cookie" or a "Local Stored Objects" feature. The "flash cookie" feature is currently used by Adobe and by Mozilla in Firefox to track visitors. You will probably want to disable these features also.

Another threat to your security when using a web browser is javascript. Javascript allows a webpage to make the browser to perform complicated functions that allow web pages to constantly change as the mouse moves around the page without the need to click on a submit button. Javascript, however, can also be used to send usernames and passwords to the wrong places, report information about your browser back to a site and install malware on your computer. For your security and privacy you may want to block javascript in your browser. The tradeoff of not using javascript is that some pages will not work properly but you will have more security.

## **Secure Email Addresses**

To secure your emails in transmission and while in storage on your computer or on third party machines you will want to encrypt your drives and follow a carefully thought out email deletion policy.

## Encrypting emails

Today there are simple and effective end-to-end encryption software tools. Two popular tools are Pretty Good Privacy (PGP) and GNU Privacy Guard which is a free tool. Both of these programs provide encryption of your emails in transit and also protect your stored emails. These products allow you to, with a click of a button, sign, verify, encrypt and decrypt email messages. By encrypting your emails their content will be protected against interception on the wire and while stored on your personal computer and on third party machines. The inconvenience of encrypting your emails is that every one you exchange the encrypted emails with will have to also use the encryption software and have keys to decrypt your messages.

If you operate a mail server make sure it supports TLS encryption when messages are sent from or to your server from another server.

If you use POP or IMAP to retrieve your email make sure it is an encrypted POP or IMAP.

Gmail also offers the option of always using HTTPS but you have to select that option on the “general” tab of the Gmail settings page. If you use a web mail service make sure you access it using HTTPS rather than HTTP.

At [SecureLaptop.org](http://www.securelaptop.org) we offer a simple, secure, and reliable email hosting service that is SSL/TLS secured, always uses HTTPS and supports end to end encryption applications. You can learn more about what this includes here: <http://www.securelaptop.org/secure-e-mail.html>

## Email Data Retention and Deletion Policy

Make sure your email is configured to delete messages off of your internet service provider’s server after you download the messages. This is the default setting if you are using POP to fetch your mail but if you are using IMAP or web mail make sure you delete messages after you read them. Even if you delete a message immediately it could be months before the message is deleted from the third party storage. The content of end-to-end encrypted emails will not be assessable through a third party’s

storage although email headers will be. The most secure option is to run your own email server with an encrypted drive.

Remember even if you delete the emails from your computer and your third party providers computer they will likely still be stored on the computers of those you sent the email to and their third party providers computers and maybe on back up servers. This is another reason to encrypt messages even if you have a strict retention and deletion policy for emails you send and receive.

## **WiFi Security**

Wireless networking or WiFi is a means of connecting computers to each other and the internet through air using wireless signals. These wireless signals can be intercepted by anyone with a computer. It is likely that unencrypted wi-fi communications enjoy no legal protections from government interception since there is no expectation to privacy when you transmit unprotected information through the air.

You can protect your wireless communications from others with WEP (wired Equivalent Privacy or WPA (Wi-Fi Protected Access) encryption software. WEP is not a strong encryption software but is worth the trouble to install to ensure your communications at least enjoy the legal protections accorded to communications exchanged with the expectation of privacy. WAP is much stronger but still is not an end-to-end encryption application. If you are using someone else's open unencrypted wireless access point like a coffee shop wireless connection you should use your own encryption tools.

## **Protecting Against Malware**

Malware refers to software that runs on a computer and operates against the interests of the computer's owners. Viruses, worms, Trojan horses, spyware and key loggers are all types of malware. Malware is spread by exploiting defects in software to give someone else control of your computer or by tricking the computer user into running a software program that does something other than what the user intended.

Malware is a high security and privacy risk. Malware may steal account details and passwords, read documents on a computer, defeat attempts to access the internet anonymously and even using your computer's microphones or webcam to spy on you. The majority of malware is designed to pop up advertisements or hijack a computer to send spam however it can be used by your adversaries for more serious invasions of your privacy. Malware run by law enforcement to collect your personal information is possible but less likely than malware used by those seeking to steal your identity for financial gain or to send spam.

The risk that your computer will be infected with malware is quite high unless a skilled computer security expert has secured the system.

## **Reduce the Risk of Malware**

The majority of malwares are targeted at Windows operating systems so operating on any other system reduces your risk of being infected. Regularly updating your software to ensure defects that are discovered are repaired is helpful. Never running software of unknown origin is the best way to avoid being tricked into installing malware. Limiting the number of users on a computer with sensitive information is helpful. And most importantly running antivirus and antispyware software will help protect against most malware. The bet is to hire a skilled computer security expert to secure your computer.

## **Using Tor to Hide Your IP Address**

Tor is a software application that bounces your internet communications around a network or servers providing anonymity. Because the signal is bounced off many nodes the site you are communicating with never sees your actual IP address. Tor is used primarily to frustrate traffic analysis. You can find installation instructions and download Tor software at <http://www.torproject.org>.

While Tor helps establish anonymity it will not protect you against malware. Be aware there are applications that are not compatible with Tor and if you use those applications

Tor will not offer any protections. Tor will also not work to deter a sophisticated surveillance monitoring. For example, surveillance that searches many sites around the internet and looks for patterns across them.

Any protection is only as good as its weakest link and Tor's weak link is its node operators. The TOR node operators are volunteers and there is no guarantee that an individual exit node operator won't hijack your information. It is recommended you use Tor with encryption software for maximum security.

## **Secure Virtual Private Networks (VPN)**

A virtual private network connects certain computers with encrypted transmissions so only those with a key to unlock the encryption can see what is being transmitted. The network of computers is not physically connected by cables rather the computers are connected by secure internet transmissions.

A VPN is easy to set up and maintain and every transmission sent from a computer in the network is encrypted. The VPN does all the coding and decoding for you. A VPN also hides your IP address when you leave the network and use Google or any other online search engine. Creating a VPN is easy and will protect you from competitors, the government, criminals, telecom operators or anyone else accessing sensitive information.

**To find out more about setting up an offshore and untraceable VPN, protected by 3 different companies in 3 different jurisdictions - SecureLaptop.org has your solution. Visit us at: <http://www.securelaptop.org/encrypted-vpn.html>**

## **Secure Virtual Over internet Protocol (VoIP)**

VoIP routes your phone calls over the internet rather than through telephone lines. There are many VoIP providers, Vonage being one of the largest and most well known. All you need to establish a VoIP is a high-speed internet connection and a phone. With any VoIP provider you enjoy the advantages of unlimited calling to landlines for less than traditional phone services and portability of your telephone number to any location.

Secure VoIP's offer these advantages plus encryption software to ensure secure communication of sensitive information.

**At SecureLaptop.org we offer a number of different plans to establishing and maintaining a high grade secure VoIP network for your organization or business. Visit us at: <http://www.securelaptop.org/secure-voip.html>**

## **Personal Security Consulting**

At SecureLaptop.org we understand that your privacy and security is of utmost concern. Preserving your wealth, private data, and personal information cannot be taken too lightly. If you did not see specifically mentioned in this report the kind of services you require, please contact us for some one on one personal security consulting. We offer a number of exclusive services to our clients and can provide you with a custom security plan, from securing your data and communications to securing your assets offshore in corporations and trusts.

**Learn more about our private security consulting options here: <http://www.securelaptop.org/security-consulting.html>**

## Conclusion

In this day and age our privacy, data security, and asset protection cannot be given enough importance. Every day our liberties and rights to privacy are being signed away in the name of “the greater good.” Malicious individuals are seeking to steal, violate, and hack their way into your personal life. Governments are spying on every move their citizens are making.

Only you can take your security into your own hands and ensure that you are completely safe from all such attacks. Education is your best weapon. We at SecureLaptops.org can provide you with the means to implement a personal and custom made security plan to suit virtually any situation. With our services you can rest assured that you, your family, and your assets are as protected as possible.